Kolaborasi *Intrusion Detection System* Berbasis *Publish/Subscribe*

Samsul Arifin dan **Endang Setyati**
Dosen STMIK AsiA Malang

ABSTRAK

Ketergantungan manusia akan teknologi informasi terus meningkat seiring dengan berjalannya waktu. Memang dengan teknologi informasi segalanya menjadi lebih cepat, praktis, dan relatif sangat mudah, jarak yang begitu jauh bermil-mil akan terasa begitu dekat. Bersama dengan itu pula maka masalah baru pun akan muncul yaitu mengenai keamanan jaringan. Salah satu faktor yang menjadi ancaman dalam keamanan jaringan adalah adanya penyusup atau attacker. Attacker akan menyusup ke dalam jaringan secara tiba-tiba tanpa sepengetahuan dari admin jaringan. Bermacam-macam tujuan dari attacker mungkin hanya sekedar iseng, melihat-lihat data atau mengambilnya bahkan akan menjadi sangat berbahaya kalau sampai merusak data dan system.

Berawal dari masalah diatas maka pada makalah ini akan membahas tentang bagaimana membuat system keamanan jaringan dengan menggunakan kolaborasi snort IDS (Intrution Detection System)dan IPtables firewall berbasis publish/subscribe. Snort dan IPtables masing-masing akan saling bekerja sama untuk mendeteksi adanya penyusup dan berusaha untuk mencegahnya masuk kedalam jaringan. Karena ada banyak host dalam jaringan maka digunakan mekanisme publish/subscribe dengan tujuan pada saat salah satu host mendeteksi adanya serangan maka akan segera dikirimkan ke topic server untuk disebarkan keseluruh host dalam jaringan, sehingga setiap host dapat mencegah penyusup untuk melakukan eksploitasi.

Kata kunci*: snort IDS, iptables firewall, publish/subscribe, elvin router*

ABSTRACT

Dependency of information technology man would be increasing along with run of time. Of course with anything information technology becomes quicker, practical, and relative hardly easy, distance which so far bermil-mil will felt so near. Together with that also hence new problem also will emerge that is about network security. One of factor becoming threat in network security is existence of infiltrator or attacker. Attacker will infiltrate into network suddenly without the knowledge from admin network. All kinds of intention of possible attacker just fad, looks around data or takes it is even will become very dangerous if unwillingly destroying data and system.

Beginning of from problem to hence at this handing out will study about how making system network security by using snort IDS (Intrution Detection System)and IPtables firewall bases on publish/subscribe. Snort and IPtables each would be each other cooperate to detect existence of infiltrator and tries to prevent it admission in network. Because there is many host in network hence applied by mechanism of publish/subscribe with a purpose to at the time of one of host detects existence of attack hence would soon is sent to topic server to be propagated for all host in network, so that every host can prevent infiltrator to do exploitation

Keywords: *snort IDS, iptables firewall, publish/subscribe, elvin router*

PENDAHULUAN

Segala kegiatan manusia sekarang ini seakan tidak pernah lepas dari teknologi informasi. Praktis, cepat dan relatif sangat mudah itulah yang menjadi alasan utama dipilihnya teknologi informasi. Seiring dengan perkembangan teknologi informasi yang begitu luas maka semakin banyak pula dampak negatif yang ditimbulkan, salah satunya yaitu *attacker* atau penyusup dalam jaringan. *Attacker* menyusup dalam jaringan secara tiba-tiba tanpa sepengetahuan dari Admin jaringan. Bermacam-macam tujuan dari *attacker* menyusup ke dalam jaringan mungkin hanya sekedar iseng atau mengambil data bahkan yang bisa menjadi sangat berbahaya bila sampai merusak data ataupun system. Oleh karena itu untuk mencegah hal-hal yang dapat merugikan maka kita harus memasang suatu system keamanan dalam jaringan kita yaitu dengan menggunakan IDS (*Intrusion Detection System)*, sedangkan model komunikasi yang digunakan adalah *system publish/subscribe.* IDS merupakan suatu teknik untuk mendeteksi adanya suatu kejanggalan dalam suatu jaringan atau system, sedangkan system *publish/subscribe* adalah metode komunikasi diantara komponen-komponen *software* atau aplikasi-aplikasi dimana ketika aplikasi diperlukan untuk menerima beberapa *message*. Dari permasalahan diatas maka akan disusun proyek akhir untuk membangun sebuah *security* jaringan dengan menggunakan IDS dan *IPtables firewall* berbasis *publish/subscribe*.

Tujuan dari penyusunan proyek akhir yang berjudul "Kolaborasi *Intrusion Detection System* Berbasis *Publish/subscribe*" ini adalah:

1. Untuk membangun suatu system keamanan jaringan dengan menggunakan snort IDS dan *iptables firewall* berbasis *publish/subscribe.*
2. Sebagai sarana pembelajaran untuk pengembangan selanjutnya menjadi lebih baik.

Dari latar belakang yang telah diuraikan dapat diambil permasalahan sebagai berikut:

1. Bagaimana mengintegrasikan IDS dan iptables firewall ke dalam sebuah system jaringan agar dapat mendeteksi adanya penyusup dan juga memblokirnya?
2. Bagaimana sebuah IDS dapat membedakan data serangan atau bukan dan mengirimkannya ke sebuah *server* agar dapat disebarkan ke seluruh *host* bahwa dalam jaringan terjadi serangan?
3. Bagaimana membangun system *publish /subscribe* untuk penyebaran informasi penyerangan yang terjadi dalam jaringan?

Dalam proyek akhir ini juga dimasukkan beberapa batasan masalah sebagai berikut:

1. Proyek akhir ini diimplementasikan pada LAN (*Local Area Network*).
2. Sistem Operasi yang digunakan adalah Linux Debian Etch.
3. IDS yang diimplementasikan adalah snort dan portsentry.
4. *Publish/subscribe* menggunakan mekanisme *Elvin router.*
5. Bahasa pemrograman yang digunakan adalah *Java.*

KAJIAN TEORI

1. IDS (*INTRUSION DETECTION SYSTEM*) DAN *FIREWALL*

Intrusion Detection System merupakan suatu aplikasi atau tools yang digunakan untuk mendeteksi adanya suatu kejanggalan dalam suatu system jaringan yang disebabkan oleh adanya penyusup dalam jaringan. Dilihat dari cara kerja dalam menganalisa apakah paket dianggap sebagai penyusupan atau bukan, IDS dibagi menjadi 2: *knowledge based* atau *missue detection* dan *behavior based* atau *anomaly based*. *Knowledge based* IDS dapat mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan database rule IDS yang berisi *signatures* paket serangan. Jika paket data mempunyai pola yang sama atau setidaknya dengan salah satu pola di database rule IDS, maka paket tersebut dianggap sebagai serangan. Demikian juga sebaliknya, jika paket data tersebut sama sekali tidak mempunyai pola yang sama dengan pola di database rule IDS, maka paket data tersebut dianggap bukan serangan.

Sedangkan behavior based atau anomaly based dapat mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan-kejanggalan pada system, atau adanya penyimpangan-penyimpangan dari kondisi normal, sebagai contoh ada penggunaan memori yang melonjak secara terus menerus atau ada koneksi parallel dari satu buah IP dalam jumlah banyak dan dalam waktu yang bersamaan. Kondisi-kondisi diatas dianggap kejanggalan yang kemudian oleh IDS jenis *anomaly based* dianggap sebagai serangan.

Dilihat dari kemampuan mendeteksi penyusupan pada jaringan, IDS dibagi menjadi 2 yakni: *host based* dan *network based*. *Host based* mampu mendeteksi hanya pada host tempat implementasi IDS, sedangkan *network based* IDS mampu mendeteksi seluruh host yang berada satu jaringan dengan host tempat implementasi IDS.

Firewall sebenarnya lebih tepat disebut sebagai *paket filter* karena fungsi utamanya adalah untuk memilih paket-paket mana saja yang boleh keluar dan masuk ke jaringan.

2. SNORT

Snort merupakan IDS *open source* yang telah menjadi standart IDS di industri. Snort dapat bekerja dalam 3 mode: *sniffer mode* (penyadap), *packet logger* dan *network intrusion detection mode*. Tentunya mode kerja yang akan digunakan dalam membangun system pencegahan penyusupan ini dalam mode kerja *network intrusion detection*. Penyusupan didefinisikan sebagai kegiatan yang bersifat *anomaly, incorrect atau inappropriate* yang terjadi di jaringan atau di *host*

a. PORTSENTRY

Portsentry adalah sebuah perangkat lunak yang dirancang untuk mendeteksi adanya *port scanning* dan merespon secara aktif bila ada port scanning. *Port scan* adalah langkah paling awal sebelum melakukan penyerangan. Cara kerja portsentry dengan melakukan melihat komputer yang melakukan *scan* dan secara aktif akan memblokir mesin penyerang agar tidak dapat masuk dan melakukan transaksi dengan server kita.

b. IPTABLES

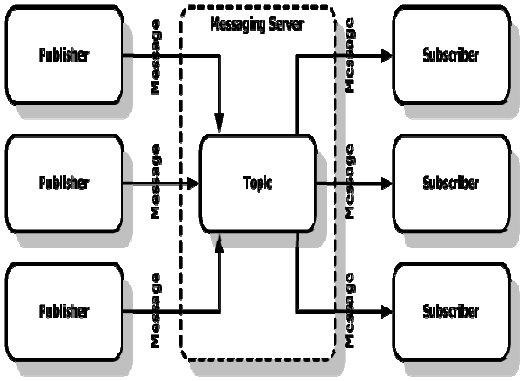
IPTables merupakan *firewall* bawaan *Linux.* Iptables mampu melakukan *filtering* dari *layer transport* sampai *layer physical*. Sebagai contoh rule dalam sebuah firewall akan menutup semua koneksi kecuali ke port 80 protokol TCP, atau sebuah rule firewall mendefinisikan bahwa yang dapat melakukan koneksi hanya paket data yang berasal dari MAC *address.*

c. PUBLISH/SUBSCRIBE MESSAGING

Messaging adalah suatu metoda komunikasi diantara komponen-komponen *software* atau

aplikasi-aplikasi. Sebuah messaging system merupakan fasilitas *peer-to-peer*; sebuah messaging client dapat mengirim *message* ke client lain dan dapat juga menerima *message* dari *client* yang lain. Masing-masing client dikoneksikan ke sebuah *messaging agent* yang memberikan fasilitas untuk membuat, mengirimkan, menerima dan membaca message.

Ketika aplikasi diperlukan untuk menerima beberapa *message*, *Publish-Subscrib Messaging* digunakan. Konsep utama dari *Publish-SubscribMessaging* adalah *Topic (messaging server).* Beberapa *Publisher* boleh mengirim *message* ke *Topic(Messaging Server)* dan seluruh *Subcriber* menerima *message* yang dikirim oleh *Topic*. Model ini diperlihatkan gambar. 1. Secara ekstrim *Publish-SubscribMessaging* ini berguna ketika sebuah group aplikasi ingin memberitahukan kepada setiap anggota group sebuah kejadian yang khusus.



Gambar 1. *Publish-Subscribe Based Messaging System*

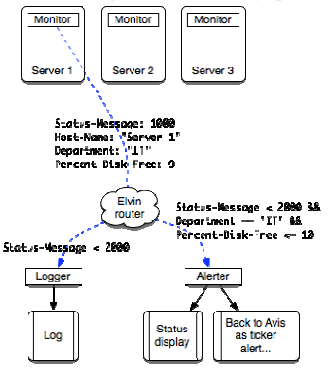
Yang perlu digaris bawahi dalam *Publish-SubscribMessaging* adalah bahwa boleh mempunyai banyak pengirim dan penerima

d. ELVIN ROUTER

Avis merupakan multicast bus data. Avis menyediakan kecepatan publish/subscribe service routing yang kompatibel dengan implementasi dikomersilkan Elvin yang dikembangkan oleh *Mantara Software.*

Elvin router dapat saling disatukan bersama-sama untuk membentuk jaringan komunikasi yang luas. Client-client dapat saling bertukar pesan dengan client yang lain dimanapun pada jalur penerimaan data dengan menggunakan ekspresi-ekspresi aturan yang sesuai saat memilih pesan-pesan yang didasarkan pada isinya.

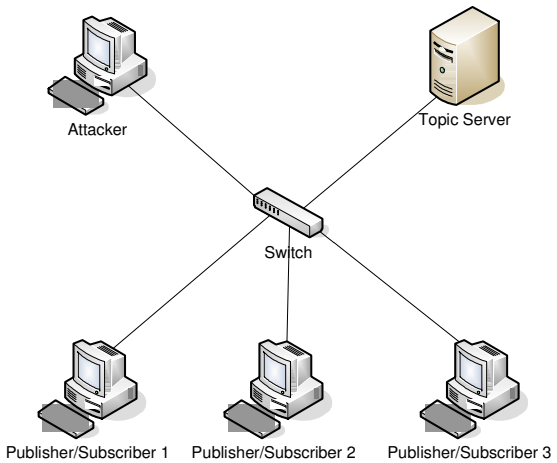
Penggunaan saat ini Elvin router telah menambahkan didalamnya suatu bus pesan untuk pemberitaan instan dan kehadiran, penemuan alat dan koordinasi ruang rapat yang baik dan sebagai pembawa dari transkripsi suara. Implementasi yang telah dikomersilkan yang dikembangkan oleh Mantara telah digunakan secara ekstensif transaksi keuangan dalam jumlah besar. Berikut ini adalah skenario contoh sederhana menggunakan Avis sebagai gambaran bagaimana mengoperasikannya.



Gambar 2. *Skenario Implementasi Elvin Router*

1) *Monitor*
   Server 1, server 2, server 3 adalah bertindak sebagai monitor dalam hal ini disebut sebagai Publisher. Terlihat pada contoh diatas server 1 mengirimkan pesan. Pesan tersebut dideskripsikan host name, departement, dan persent disk free. Informasi yang dikirimkan oleh server 1 yaitu :
   Status-Message = 1000
   Host-Name = "Server 1"
   Departement = "IT", Persent Disk Free = 9.
2) *Logger*
   Setiap ada host yang mengirimkan status message maka akan dilakukan proses logger dalam suatu log file.
3) *Alerter*
   Alerter disini disebut sebagai Subscriber yang akan menerima message dari server yang mengirimkan pesan. Alerter mempunyai rule untuk menerima pesan yaitu :
   Status-Message < 2000 &&
   Departement = = 'IT' &&
   Persent-Disk-Free <= 10

PEMBAHASAN



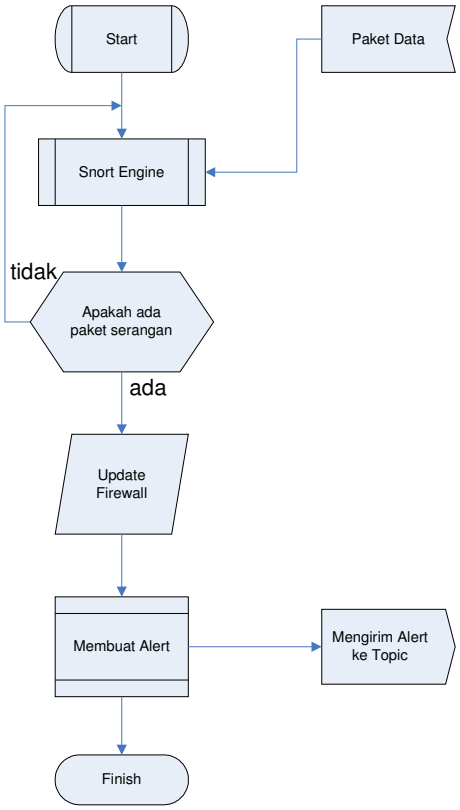
Gambar 3. *Topologi Jaringan yang digunakan*

Dalam bab ini akan dibahas mengenai tahap-tahap perancangan dan pembuatan Kolaborasi *Intrusion Detection System* Berbasis *Publish /Subscribe.* Implementasi dari aplikasi ini adalah untuk LAN (*Local Area Network*). Dalam satu jaringan ini akan terdapat empat buah host sebagai Publisher maupun Subscriber dan satu server sebagai Topic Server. Jaringan ini akan terhubung dengan jaringan yang lain melalui sebuah router dimana akan dilakukan penyerangan (*Attacke*r) dari jaringan yang lain. Adapun gambaran umum mengenai sistem yang akan dibuat adalah seperti gambar berikut ini:

1. Perancangan Sistem

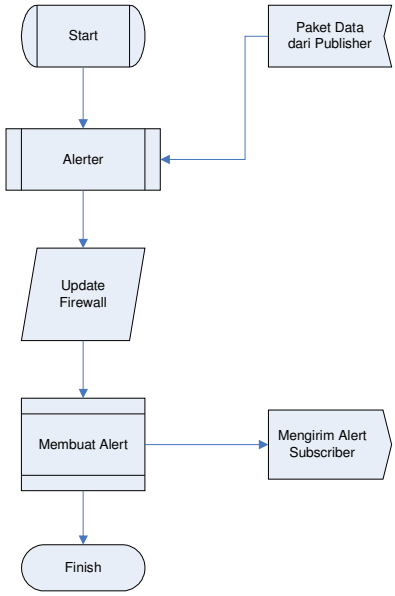
Pada tahap ini akan dibuat desain sistem yang meliputi: pembuatan sistem publish /subscribe kemudian di integrasikan dengan IDS dan iptables.

Berikut merupakan flowchart untuk proses publisher, subscriber dan topic server pada saat menemukan ada serangan dalam jaringan.



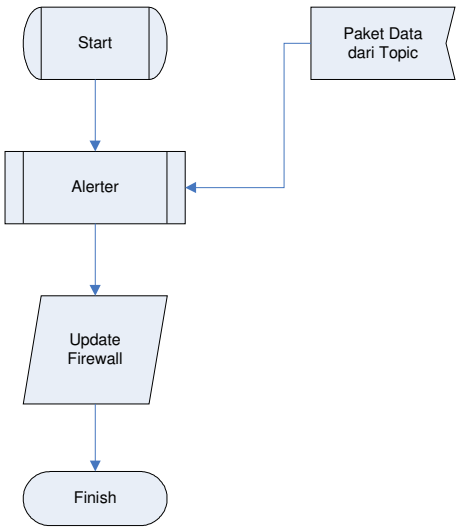
Gambar 4. *Flowchart pada Publisher*

Flowchart diatas merupakan proses yang terjadi pada Publisher. Saat ada paket data yang datang maka portsentry ataupun snort akan melakukan pengecekan yaitu dengan mencocokan paket yang datang dengan signature database rule snort. Bila ditemukan ada paket yang sama dengan database rule snort maka paket tersebut akan segera diblok, dan kemudian publisher akan mengirimkan alert ke Topic server.



Gambar 4. *Flowchart pada TopicServer*

Flowchart diatas merupakan proses yang terjadi pada topic server. Paket data dari publisher akan diterima oleh alerter yang digunakan untuk melakukan update firewall. Setelah itu Topic server akan membuat paket data untuk disebarkan ke seluruh subscriber.



Gambar 5. *Flowchart padaSubscriber*

Flowchart diatas merupakan proses yang terjadi pada subscriber. Paket data dari topic server akan diterima oleh alerter kemudian iptables akan melakukan eksekusi sesuai dengan paket data yang diterima dari Topic server.

2. Pengujian Dan Analisa

Pada pengujian tahap ini langkah-langkah yang harus dilakukan adalah sebagai berikut:

a. Pengujian Pada Topic Server

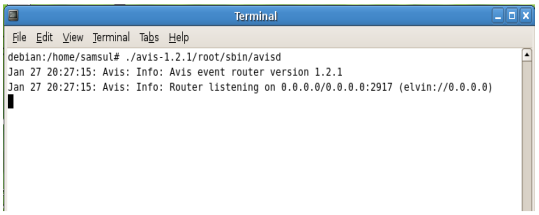
Pengujian pada topic server digunakan untuk mengetahui apakah elvin route sudah berfungsi dengan baik atau belum. Berikut langkah-langkah pengujian pada topic server:

Login sebagai root kemudian jalankan elvin router

|./home/...../avis-1.2.1/root/sbin/avisd

|Jan 20 14:53:36: Avis: Info: Avis event router |version 1.2.1

|Jan 20 14:53:38: Avis: Info: Router listening on |0.0.0.0/0.0.0.0:2917 (elvin://0.0.0.0)



Gambar 6. Elvin Router sedang running

Gambar 6. menunjukkan bahwa elvin router sudah berjalan dengan baik dan secara default elvin router akan menerima request dari Local Area Network (LAN).

b. Pengujian Pada Publish/Subscribe

Analisa publish/subscribe dilakukan dengan menggunakan metode Trial and Error. Pada pengujian tahap ini langkah-langkah yang akan dilakukan adalah sebagai berikut:

Proses Hacking

Proses hacking ini adalah untuk mengetahui berhasil tidaknya sistem IDS yang telah dibuat, berhasil tidaknya IDS ditentukan dari kemampuan sistem untuk mengalihkan dan mencatat serangan ke log file. Jenis hacking yang digunakan untuk menganalisa konfigurasi sistem IDS ini adalah

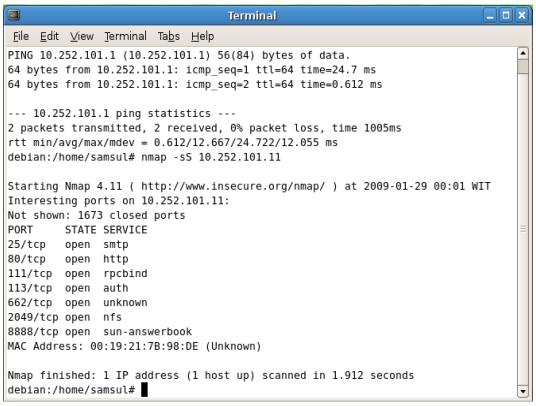
a. *Nmap*
b. *7th sphere edition*
c. *TFTP Bruteforce*
d. *IIS Exploit*

Pengujian dan Analisa IDS terhadap serangan

Analisa terhadap Nmap

Nmap adalah sebuah program open source yang berguna untuk mengeksplorasi jaringan. Nmap didesain untuk dapat melakukan scan jaringan yang besar, juga dapat digunakan untuk melakukan scan host tunggal. Nmap menggunakan paket IP untuk menetukan host-host yang aktif dalam suatu jaringan, port-port yang terbuka, sistem operasi yang digunakan, tipe firewall yang dipakai dll.

Lakukan nmap mode biasa dari komputer penyerang menuju host target

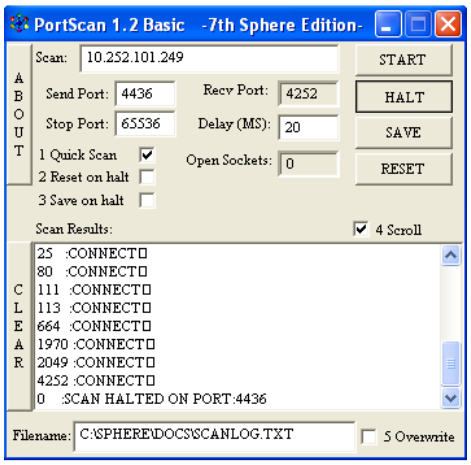


Gambar 7. *Melakukan Scanning port dengan Nmap*

Langkah selanjutnya melihat apakah serangan tersebut dapat dideteksi oleh IDS dengan rule-rule yang dimilikinya dan mencatat hasil intrusi ke log IDS. Dibawah ini adalah potongan log dari snort seketika setelah ada koneksi dari attacker yang berusaha melakukan scanning port.

Analisa terhadap 7th sphere edition

7th sphere edition adalah sebuah tools yang digunakan untuk melakukan scanning port dengan mudah dan cepat. Dibawa ini tampilan yang terdapat pada attacker. Cobalah lagi melakukan scanning port dengan 7th sphere edition.



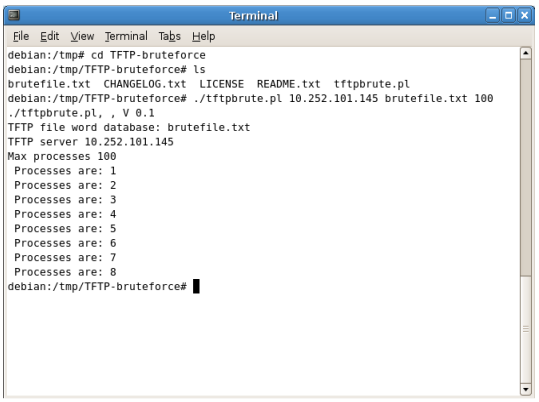
Gambar 8. *Scanning Port dengan 7th sphere edition*

Gambar 4.9. menunjukkan bahwa attacker melakukan scanning ke *host target* dengan IP 10.252.101.249.

Berikut log yang dihasilkan oleh IDS dari percobaan scanning port dengan menggunakan 7th sphere edition.

Analisa terhadap TFTP *BruteForce*

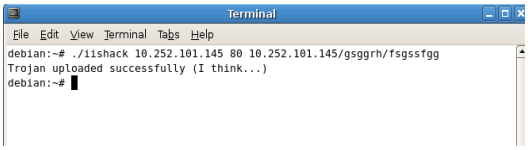
Langkah berikutnya adalah melakukan percobaan dengan menggunakan TFTP BruteForce. Jalankan TFTP BruteForce sebagai attacker



Gambar 9. *Proses eksploit dengan TFTP BruteForce*

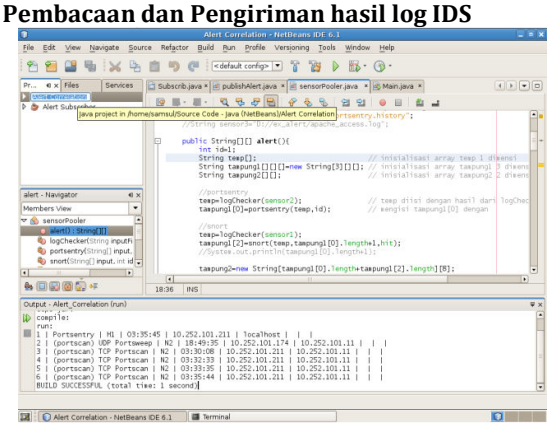
Dari percobaan penyerangan seperti diatas kita akan dapat mengetahui bagaimana suatu IDS dapat mendeteksi suatu serangan exploit berikut adalah hasil log dari IDS

Analisa terhadap IISExploit



Gambar 10. *Proses attack dengan IISExploit*

Pembacaan dan Pengiriman hasil log IDS

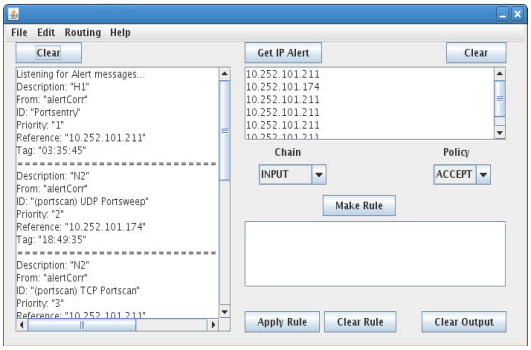


Gambar 11. *Pembacaan dan Pengiriman alert oleh Publisher.*

Penerimaan log IDS *(Subscriber)*

1. Nmap

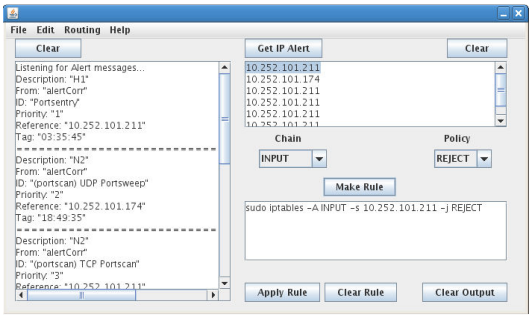
Subscriber akan menerima pesan alert tadi dari publisher yang berupa informasi jenis serangan IP penyerang dan lain-lain.



Gambar 12. *Subscriber menerima alert dari Publisher*

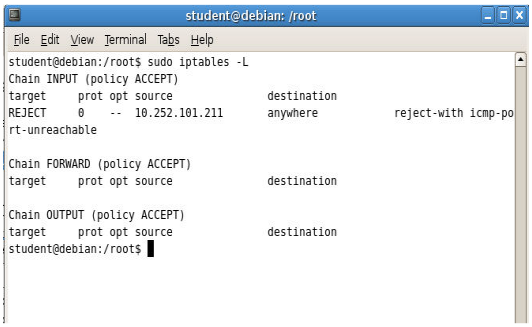
Update Firewall

Setelah mendapat IP dari attacker maka tujuan kita selanjutnya adalah melakukan bloking dengan firewall. Pilih IP yang ingin dimasukkan dalam rule firewall kemudian tentukan CHAIN dan POLICY.



Gambar 13. *Menbuat rule firewall*

Setelah membuat *rule firewall* maka tinggal menekan tombol ***apply rule***, lalu periksa rule iptables pada terminal apakah sudah ter-update



Gambar 14. *Melihat isi Rule dari Iptables*

Analisa Hasil Pengujian

		NMAP	7th sphere edition	TFTP Brute force	IIS-eksploit
Snot	Logging	√	√	√	√
	Tidak	-	-	-	-
Portsentry	Logging	√	√	√	-
	Tidak	-	-	-	√

PENUTUP

Berdasarkan hasil pengujian dan analisa yang telah di bahas pada bab sebelumnya maka dapat diberikan beberapa kesimpulan sebagai berikut :

1. Snort bekerja dengan cara mendeteksi setiap paket data yang masuk kedalam jaringan kemudian membandingkannya dengan rule database.
2. Dianggap sebagai sebuah serangan atau bukan tergantung dari signature database snort. Bila sebuah paket memiliki header yang sama dengan rule database maka dianggap sebagai serangan.
3. Percobaan serangan dilakukan dengan menggunakan metode Nmap, Dos Attack, Network sniffing, yang mana snort dapat melakukan pendeteksian dan iptables dapat memblokirnya.
4. Elvin router dapat bekerja dengan baik, dapat menerima dan mengirimkannya ke semua host dalam jaringan.

Sebagai saran yang dapat diberikan yaitu :

Untuk pembacaan log snort dapat dibuat lebih kompleks lagi, karena hasil log snort mempunyai banyak karakter.

DAFTAR PUSTAKA

1. Hermana, Asep Nana, 2003. " *Membangun Messaging Service yang Aman*" Tugas Besar Keamanan Sistem Informasi- ITB.
2. http://avis.sourceforge.net
3. Snort™Users Manual The Snort Project 2006.
4. IPTables Manual.
5. Purbo, Onno W. " *Portsentry Penjaga Serangan Port Scan di Jaringan"*
6. Hartono, Puji. " *Sistem Pencegahan Penyusupan pada Jaringan Berbasis Snort IDS dan IPTables Firewall"*. Tugas Kuliah Keamanan Sistem Lanjut. 2006
7. http://netbeans.org
8. http://java.sun.com

(Tolong di tanyakan ke penulis, judul buku yang belum ada tahun terbitnya, nama penerbit dan kotanya)